REMARKS

In response to the Office Action dated April 15, 2009, Applicant respectfully requests reconsideration and withdrawal of the rejections of the claims. Claims 1 to 15 have been replaced by new claims 16 to 30. Support for the claim amendments can be found in the specification, for example at pp. 6-11, as well as in FIGs. 1 and 2. Claims 16 to 30 are pending.

I. **Claim Rejections - 35 U.S.C. § 112**

Claims 1 to 15 were rejected under 35 U.S.C. § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Without conceding to the propriety of the rejection, to remove this issue Applicant has replaced claims 1 to 15 with new claims 16-30. Applicant respectfully submits that claims 16-30 comply with the requirements of the statute.

II. **Claim Rejections - 35 U.S.C. § 102**

Claims 1 to 15 were rejected under 35 U.S.C. § 102(b) as being anticipated by U.S. Patent Publication No. 2002/0069361 to Watanabe et al. ("*Watanabe*").

Watanabe discloses a public key certificate system for identifying a communicating party on the other end in data communication via a medium or a communications network such as the Internet. (*Watanabe*, paragraph 21). The authentication of a person is realized using a person identification certificate (IDC). An IDC is issued for each person who wants to be certified by an identification authority (IDA), a third-party agency, after verifying the identification of the person.

(*Watanabe*, paragraph 155). Each IDC includes template information which identifies a corresponding person. Such information includes fingerprint information, retina pattern information, iris pattern information, voice print information, and handwriting information. Furthermore, a combination of a password and template information may also be used. (*Watanabe*, paragraph 156). As such, an IDC issued by an IDA is used to authenticate a user. (*Watanabe*, paragraph 157). *Watanabe* discloses the IDC, including the template information, is stored and encrypted in various ways. (*Watanabe*, paragraphs 225-234).

In one of *Watanabe*'s numerous examples, an IDC is used to identify a particular user who is authorized to use a device (such as a PC). (*Watanabe*, paragraph 237). Here, a public key of a user or a user device is used to encrypt a template. When a user wants to use a PC, the template stored in the IDC is decrypted using the private key of the user and is compared with an input template to verify the authenticity of the user. (*Watanabe*, paragraph 237). *Watanabe* discloses several examples of configurations and systems that may be used to verify the identity of a user. (*Watanabe*, FIGs. 19-20 and 25-27).

In one example, Figure 19 shows that a user device or the service provider 300 has a sampling information processing unit 310 for acquiring personal information, such as fingerprint data, of various users and processing the acquired information. The information processing unit 310 has a personal information acquisition unit 314 for acquiring sampling information and an information converter 313 for converting fingerprint data into code. The user device includes a communication unit 312 for transmitting converted code to an IDA 320. Moreover, the sampling information processing unit 310 stores a public key certificate for use in encryption/decryption of data in various communication processes. (*Watanabe*, paragraph 281).

IDA 320 then compares sampling data received from the user device with a template stored in the IDA. (*Watanabe*, paragraph 282). When the comparison is performed, the result, an OK message or an NG message, is transmitted to the user device depending on whether the received sampling information matches the stored template. (*Watanabe*, paragraph 284).

Turning to the claimed invention, claim 16 recites, *inter alia*, "storing said encrypted authentic biometric signature on a computer associated with said piece of equipment." Unlike the claimed invention, *Watanabe*'s user device does not store the encrypted authentic biometric signature; rather, the template information is stored at the IDA. It is beneficial to store an encrypted biometric signature on a computer associated with a piece of equipment in order to prevent hackers from compromising such information and gaining access to a piece of equipment. Since *Watanabe* does not disclose the above-identified features of claim 16, it cannot support a rejection of claim 16 under 35 U.S.C. §102(b).

In an another example in *Watanabe* shown in Figure 20, the user device 400 additionally includes a template decryption unit that decrypts the template stored on the IDA and performs the comparison between the sampling data received from the user device and the decrypted template in the comparator 416.

Claim 16 recites, *inter alia*, "decrypting, **in said authentication medium**, said encrypted authentic biometric signature stored on said computer" and "verifying, **in said authentication medium**, the authenticity of said plain biometric signature by comparing said plain biometric signature of said user with said decrypted authentic biometric signature of said authorized user." (Emphasis added). Unlike the claimed invention, *Watanabe*'s user device performs the decryption of the template and the comparing between the sampling data received from the user device and the decrypted template. Since *Watanabe* does not disclose the above-identified features of claim 16, it cannot support a rejection of claim 16 under 35 U.S.C. §102(b).

In another example, *Watanabe* discloses a system in which verification is performed by transmitting an IDC stored in an IC card to a shared user device, such as a PC. (*Watanabe*, FIG. 25 and paragraphs 344-347).

Claim 16 recites, *inter alia*, "decrypting, **in said authentication medium**, said encrypted authentic biometric signature stored on said computer" and "verifying, **in said authentication medium**, the authenticity of said plain biometric signature by comparing said plain biometric signature of said user with said decrypted authentic biometric signature of said authorized user." (Emphasis added). Unlike the claimed invention, *Watanabe*'s user device performs the decryption of the template and the comparing between the sampling data received from the user device and the decrypted template. Since *Watanabe* does not disclose the above-identified features of claim 16, it cannot support a rejection of claim 16 under 35 U.S.C. §102(b).

In another example, *Watanabe* discloses a system in which verification is performed by decrypting an IDC stored in an IC card and then transmitting the decrypted IDC to the shared user device, such as a PC, where the template information is compared to the information acquired from the identification reading unit. (*Watanabe*, FIG. 26 and paragraphs 351-353).

Claim 16 recites, *inter alia*, "verifying, in said authentication medium, the authenticity of said plain biometric signature by comparing said plain biometric signature of said user with said decrypted authentic biometric signature of said authorized user." (Emphasis added). Unlike the claimed invention, *Watanabe*'s user device performs the comparing between the sampling data received from the user device and the decrypted template. Moreover, transmitting decrypted IDC to a PC enables hackers to possibly compromise such information to gain access to a piece of equipment. Accordingly, because *Watanabe* does not disclose the above-identified features of claim 16, it cannot support a rejection of claim 16 under 35 U.S.C. §102(b).

Watanabe further discloses a system in which verification is performed by an IC card using an IDC stored in the IC card and only the result of the verification is transmitted to the shared user device, such as a PC. (*Watanabe*, FIG. 27 and paragraphs 355-357).

Claim 16 recites, *inter alia*, "storing said encrypted authentic biometric signature on a computer associated with said piece of equipment." Unlike the claimed invention, *Watanabe*'s user device does not store the encrypted authentic biometric signature; rather, the template information is stored at the IC card. It is beneficial to store an encrypted biometric signature on a computer associated with a piece of equipment in order to prevent hackers from compromising such information and gaining access to a piece of equipment. Since *Watanabe* does not disclose the above-identified features of claim 16, it cannot support a rejection of claim 16 under 35 U.S.C. §102(b).

Applicant respectfully submits that claims 17 to 20 are allowable over *Watanabe* at least due to their corresponding dependence from claim 16.

Independent claims 21 and 26, although having different scope than claim 16, recite similar distinguishing features to those recited in claim 16. Accordingly, Applicant respectfully submits claims 21 and 26 are also allowable over *Watanabe*.

Additionally, claim 21 recites, "sending said encrypted authentic biometric signature, that matches with said personal identification code, to said authentication medium." *Watanabe* lacks disclosing this feature recited in the claim. As such, Applicant respectfully submits claim 21 is allowable over *Watanabe* for at least this additional reason.

Applicant respectfully submits that claims 22 to 25 are allowable over *Watanabe* at least due to their corresponding dependence from claim 21.

Additionally, claim 26 recites, "an authentication medium having a controller, wherein said controller: receives said encrypted authentic biometric signature, associated with said personal identification code." *Watanabe* lacks disclosing this feature recited in the claim. As such, Applicant respectfully submits claim 26 is allowable over *Watanabe* for at least this additional reason.

Applicant respectfully submits that claims 27 to 30 are allowable over *Watanabe* at least due to their corresponding dependence from claim 26.

III. Conclusion

Reconsideration and withdrawal of the rejections, and allowance of all pending claims, are respectfully requested.

Respectfully submitted,

BUCHANAN INGERSOLL & ROONEY PC

Date: August 11, 2009

By: /Scott E. Jones/
Scott E. Jones
Registration No. 64392

P.O. Box 1404
Alexandria, VA 22313-1404
703 836 6620